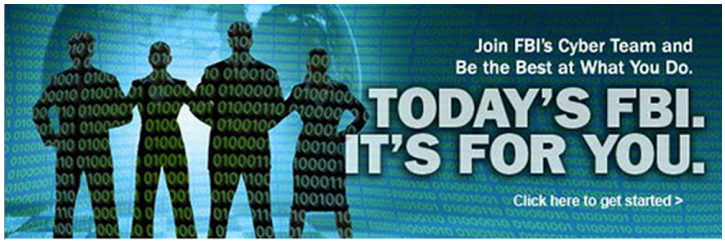
AS FBI'S AMERITHRAX CASE CONTINUES TO CRUMBLE, BUREAU DIGS IN ON NORTH KOREA CLAIMS



In ads released even as their claims about North Korea come under scrutiny, FBI tries to make cybersecurity Agents look like Eliot Ness.

Less than 10 days ago, Jim laid out yet more evidence that the FBI's claimed explanation for the anthrax attack — that USAMRIID researcher Bruce Ivins not only perpetrated the attack, but did so acting alone — was scientifically problematic. So 13 years ago, anonymous sources blamed Iraq for the attack, 12 years ago they blamed Steven Hatfill, and 6 years ago, they started blaming Bruce Ivins. Probably, none of those claims are true.

The FBI still hasn't solved one of the most alarming terrorist attacks in this country, an attempt to kill two sitting US Senators. Instead, it persists in a claim (versus Ivins) that doesn't comport with the science, to say nothing of the other circumstantial evidence. FBI only ever sustained that claim by assuming — based on no known evidence — that a Lone Wolf, rather than conspirators, launched the attack.

Even as new evidence undermining the FBI's obstinate claims about Ivins got released, the FBI has been making equally obstinate claims that North Korea is behind the Sony hack.

And then someone crashed North Korea's Internet

which, given how tiny it is, is the strategic equivalent of launching spitballs at a small group of North Korea's elite. A truly awesome use of American power!

As I noted on Salon, even as the FBI was leaking its certitude to the big press that North Korea was behind the hack, Kim Zetter was pointing out all the reasons that made no sense.

Now, with a week of holiday cheers under their belts, more of the press is beginning to note all the experts questioning the FBI's claim. Shane Harris describes the FBI "doubling down" on its original theory.

> In spite of mounting evidence that the North Korean regime may not have been wholly responsible for a brazen cyberassault against Sony—and possibly wasn't involved at all—the FBI is doubling down on its theory that the Hermit Kingdom solely bears the blame.
>
> "We think it's them," referring to the North Koreans, an FBI spokesperson told The Daily Beast when asked to respond to reports from private investigators that other culprits were responsible. The latest evidence, from the cyberanalysis firm the Norse Corp., suggests that a group of six individuals, including at least one disgruntled ex-Sony employee, is behind the assault, which has humiliated Sony executives, led to threats of terrorist attacks over the release of a satirical film, and prompted an official response from the White House.
>
> The FBI said in a separate statement to journalists on Monday that "there is no credible information to indicate that any other individual is responsible for this cyberincident." When asked whether that left open the possibility that other individuals may have assisted North Korea or were involved in the

> assault on Sony, but not ultimately responsible for the damage that was done, the FBI spokesperson replied, "We're not making the distinction that you're making about the responsible party and others being involved."

Time catalogs the alternatives to FBI's theories.

And Politico notes that when one cybersecurity company, Norse, shared its analysis, the FBI refused to share its own data, as the company had expected.

> The FBI says it is standing by its conclusions, but the security community says the agency has been open and receptive to help from the private sector throughout the Sony investigation.
>
> Norse, one of the world's leading cyber intelligence firms, has been researching the hack since it was made public just before Thanksgiving.
>
> Norse's senior vice president of market development said the quickness of the FBI's conclusion that North Korea was responsible was a red flag.
>
> "When the FBI made the announcement so soon after the initial hack was unveiled, everyone in the [cyber] intelligence community kind of raised their eyebrows at it, because it's really hard to pin this on anyone within days of the attack," Kurt Stammberger said in an interview as his company briefed FBI investigators Monday afternoon.
>
> He said the briefing was set up after his company approached the agency with its findings.
>
> Stammberger said after the meeting the FBI was "very open and grateful for our

> data and assistance" but didn't share any of its data with Norse, although that was what the company expected.

It's a bad thing, given how much evidence is out there about this hack, that the FBI won't let more of its thinking be tested publicly.

Meanwhile, in a remarkable joining of opinion, both Jack Goldsmith and Moon of Alabama note that Obama may have wasted US credibility by so quickly accusing North Korea.

And NYT's Ombud, Margaret Sullivan, admits that NYT too quickly repeated — and granted anonymity to — FBI's flimsy claims.

> [A]s a reader, Brad Johnson, noted in an email. He wrote: "Did NYT learn its lesson from the Iraq WMD debacle, or is the paper back to bad habits of writing stories from whole cloth based on anonymous White House and intelligence agency officials?"
>
> Now that the matter of who was behind the hack is coming under more scrutiny, including in The Times (though with less prominence), those kinds of questions are even more germane.
>
> One thing is certain: Anonymity continues to be granted to sources far more often than a last-resort basis would suggest.

Though Sullivan's caution didn't lead the Editorial Board to show any.

I'm glad people are now showing skepticism, even if it is too late to preserve American credibility (as if we had that anyway after StuxNet).

There's one more factor that deserves notice here: the role of cybersecurity firms in laundering government propaganda.

One of the most pregnant observations in Zetter's *Countdown to Zero Day* comes after Symantec published the first details implicating the US and Israel in the StuxNet attack. The Symantec team expected a bunch of others to jump in and start validating their work. Instead, they were met with almost complete silence. While Zetter didn't say it explicitly, the implication was that the security industry is driven by its interest in retaining the good will of the US Government. Here, the first security firm to back the North Korea claim was Mandiant, the firm that served as a surrogate for claims against China.

And while in this case there is no lack of experts willing to push back against US claims, I just wonder whether at least some of the initial credulity on the North Korea claims arose because of the dominance of USG contractors among the earliest reports on the hack? While there are some equivalents in the WMD vein, the cyberindustry, in particular, seems particularly prone to serving as a cut-out for both poorly analyzed intelligence and even propaganda.

Ah well. It's not like anyone is demanding FBI resume its hunt for the terrorist who might have killed two sitting US Senators. Why do I think this will be any different?